RANCANG BANGUN ARSITEKTUR *LIBRARY* SISTEM AUTENTIKASI ONE TIME PASSWORD MENGGUNAKAN PROSEDUR *CHALLENGE-RESPONSE*

TUGAS AKHIR

Oleh :

YUDISTIRA ARYA SAPOETRA
0534010051

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INDUSTRI - FTI
UNIVERSITAS PEMBANGUNAN NASIONAL "VETERAN "
JAWA TIMUR

2010

Nama : Yudistira Arya Sapoetra
NPM : 0534010051
Judul : Rancang Bangun Aristektur Library Sistem Autentikasi One Time Password Menggunakan Prosedur *Challenge Response*
Dosen Pembimbing 1 : Nur Cahyo W., S.Kom, M.Kom
Dosen Pembimbing 2 : Achmad Junaidi, S.Kom

ABSTRAKSI

Dewasa ini dalam berbagai bidang semakin sering ditemui penggunaan komputer yang terhubung pada jaringan. Informasi adalah aset yang paling berharga dan rahasia, berbagai cara dilakukan untuk mempertahankan aset itu dari tangan yang tidak bertanggung jawab. Selalu ada seseorang yang diberi kepercayaan penuh untuk bertanggung jawab menjaga utuhnya data dan informasi.

Bagaimana memberikan keamanan pada sebuah sistem, dari serangan dan usaha penetrasi dari luar maupun dari dalam jaringan komputer itu, yang sekarang masih banyak digunakan adalah sistem ber-password. Sistem password statis apabila sering digunakan berkali-kali maka ID login dan password akan rentan sekali terhadap bentuk serangan kedalam sistem komputer.

Untuk menghindari pencurian password dan pemakaian sistem secara ilegal, akan bijaksana bila jaringan kita dilengkapi sistem password sekali pakai. Sistem otentikasi One Time Password (OTP) adalah sistem yang menggunakan password yang berbeda disetiap user akan masuk kedalam sebuah sistem. Dari situlah diharapkan OTP dapat menjadi solusi dalam sebuah sistem keamanan jaringan. Tugas akhir ini mengimplementasikan salah satu metode sistem keamanan yang bisa digunakan sebagai solusi perlindungan komputer.

Setelah dilakukan analisis dan uji coba, maka didapat kesimpulan bahwa fungsi – fungsi yang digunakan sebagai komponen arsitektur *library* dapat berjalan dengan baik, dan sudah memenuhi prosedur *Challenge-Response*.

Kata kunci: OTP, sistem otentikasi, keamanan jaringan

KATA PENGATAR

Puji dan syukur kami panjatkan ke hadirat Allah SWT atas berkat rahmat dan karunia-Nya, sehingga dengan segala keterbatasan waktu, tenaga dan pikiran yang dimiliki penyusun, akhirnya penyusun dapat menyelesaikan Tugas Akhir yang berjudul ”**Rancang Bangun Sistem Arsitektur Library Sistem Autentikasi One Time Password Menggunakan Prosedur Challenge Response”** tepat waktu.

Tugas Akhir dengan beban 4 SKS ini disusun guna diajukan sebagai salah satu syarat untuk menyelesaikan program Strata Satu (S1) pada jurusan Teknik Informatika, Fakultas Teknologi Industri, UPN ”VETERAN” Jawa Timur.

Melalui Tugas Akhir ini penyusun merasa mendapatkan kesempatan emas untuk memperdalam ilmu pengetahuan yang diperoleh selama di bangku perkuliahan, terutama berkenaan tentang penerapan jaringan komputer. Namun, penyusun menyadari bahwa Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu penyusun sangat mengharapkan saran dan kritik dari para pembaca untuk pengembangan aplikasi lebih lanjut.

Surabaya, Juni 2010

Penyusun

UCAPAN TERIMA KASIH

Penyusun menyadari bahwasanya dalam menyelesaikan Tugas Akhir ini telah mendapat banyak bantuan dan dukungan dari berbagai pihak, untuk itu pada kesempatan yang berharga ini, penyusun mengucapkan terima kasih kepada :

1. Bapak Ir. Sutiyono, MT selaku dekan Fakultas Teknologi Industri
2. Bapak Basuki Rahmat, S.Si, MT selaku ketua jurusan Teknik Informatika
3. Bapak Nur Cahyo Wibowo, S.Kom, M.Kom selaku Dosen Pembimbing I dan Bapak Achmad Junaidi, S.Kom selaku Dosen Pembimbing II yang telah banyak meluangkan waktu dan pikiran untuk memberikan arahan dan ilmu yang berguna kepada penyusun untuk segera menyelesaikan Tugas Akhir ini.
4. Bapak Basuki Rahmat, S.Si, MT, Bapak Made Kamisutara, S.Kom, M.Kom, dan Bapak Doddy Ridwandono, S.Kom selaku penguji Skripsi yang telah banyak memberikan masukan serta membuka wawasan baru.
5. Ibunda Ir. Rini Soekmawati dan Ayahanda Ir. Agoes Wirjosapoetra terima kasih telah memberikan semangat, nasihat, ilmu, dan dukungan dalam bentuk apapun serta tiada henti mendoakan penyusun supaya Tugas Akhir ini segera terselesaikan dan menjadi orang yang berhasil, sholeh, serta berguna untuk bangsa dan negara.
6. Budhe Endang terima kasih buat do'anya, Pakdhe Koesno terima kasih buat nasihatnya, Mas Dian, Dhana, Doni siap kita maen DOTA lagi, he he he.
7. Pak Pri dan Ibu Sri (calon mertua) yang selalu memberikan semangat kepada penyusun untuk segera menyelesaikan Tugas Akhir.
8. *My Lovin'* Purna Fitri Nurliana, Amd(Keb) si Tembem yang selalu memberikan do'a, dan memberi semangat pantang menyerah, terima kasih udah setia dan sabar menunggu penyusun dalam menyelesaikan Tugas Akhir ini.
9. Special thanks for Arif Rahman Sujatmika, S.Kom, thanks banget udah meluangkan waktu, ilmu, dan tenaga.

10. Sahabat-sahabat penyusun, Wahyu Syaifullah, S.Kom (thanks ilmu - ilmunya), Gandos, Cakman, Sindu, Prast (kita Wisudha bareng), Rendy n the gang, dan semuanya yang tidak bisa penulis sebutkan satu-per-satu.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

BAB I

PENDAHULUAN

1.1 Latar Belakang

Penggunaan komputer yang terhubung ke jaringan dewasa ini semakin sering ditemui di berbagai jenis bidang maupun badan usaha. Informasi penting dan rahasia yang tersimpan pada server menjadi aset yang paling berharga pada sebuah badan usaha. Sistem keamanan komputer yang terhubung ke jaringan akan menjadi hal yang mendapat perhatian paling utama. Untuk mengamankan dokumen berupa informasi, berbagai cara dilakukan demi mempertahankan aset itu dari tangan yang tidak bertanggung jawab. Misalnya disetiap bagian dalam sebuah badan usaha selalu ada seseorang yang diberi kepercayaan penuh untuk bertanggung jawab menjaga utuhnya data dan informasi yang terdapat dalam sebuah komputer, dari serangan dan usaha penetrasi dari luar maupun dari dalam jaringan komputer itu. Karena jaringan memiliki lingkup yang cukup luas, maka dari itulah sistem autentikasi dibutuhkan untuk memilih mana user yang berhak untuk mengakses ke sebuah sistem tersebut, dan mana yang tidak berhak.

Terdapat beberapa metode untuk melakukan autentikasi, metode yang paling umum dan paling sering digunakan adalah menggunakan password statis. Tetapi apabila password statis digunakan berulang kali untuk masuk ke sebuah sistem, maka ID login dan password tersebut akan rentan terhadap *sniffer* jaringan. Salah satu bentuk serangan ke sistem komputer jaringan adalah

seseorang mencoba masuk ke dalam suatu koneksi jaringan untuk mendapatkan informasi.

Yang sekarang masih banyak digunakan adalah sistem ber-password. Untuk menghindari pencurian password dan pemakaian sistem secara ilegal, akan bijaksana bila jaringan kita dilengkapi sistem password sekali pakai. Sistem otentikasi One Time Password (OTP) adalah sistem yang menggunakan password yang berbeda disetiap user akan masuk kedalam sebuah sistem. Dari situlah diharapkan OTP dapat menjadi solusi dalam sebuah sistem keamanan jaringan.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, tulisan ini akan membahas sistem autentikasi dengan metode One Time Password:

a. Bagaimana merancang dan membangun arsitektur pada *dynamic library* yakni berisi fungsi-fungsi otentikasi one time password.
b. Bagaimana merancang dan membangun proses otentifikasi melibatkan prosedur *challenge/response*

1.3 Batasan Masalah

Adapun Batasan permasalahan pada *dynamic library* yang dibangun ini adalah :

a. Digunakan pada lingkup *local area network*
b. Komputer yang berhak mengakses telah di masukkan di dalam database

c. Hanya dapat melindungi system dari serangan pasif

d. Maksimum karakter key 6 karakter

e. Hanya dapat berjalan pada Sistem Operasi Windows XP

1.4 Tujuan Penelitian

Tujuan dari penelitian ini antara lain adalah :

a. Membangun komponen *dynamic library* one time password

b. Menerapkan Metode *Challenge Response* pada sistem autentikasi

1.5 Manfaat Penelitian

Manfaat dari penelitian ini diharapkan dapat bermanfaat bagi:

a. Memudahkan programmer dalam membangun system login dengan tingkat keamanan yang baik.

b. Dengan adanya komponen ini, maka programer dapat menerapkan atau menggunakan sesuai dengan kebutuhan.

1.6 Metodologi Penulisan

Tugas Akhir dan penelitian lapangan ini diselesaikan dengan menggunakan urutan metodologi sebagai berikut :

a. *Study literature*

   Study literature dilaksanakan dengan cara mengumpulkan dan mempelajari segala macam informasi yang berhubungan dengan Sistem Keamanan pada jaringan, dan segala hal yang berhubungan dengan model pemrogramannya.

b. Desain Sistem

Pada tahap ini dilaksanakan perancangan Sistem Perangkat Lunak yang akan dibuat berdasarkan hasil *study literature* yang ada. Perancangan komponen library ini meliputi desain arsitektur, desain struktur data, desain aliran informasi, desain algoritma dan pemrograman. Perencanaan penggunaan bahasa pemrograman

c. Analisis dan Perancangan Sistem

Dalam tahap ini, dilakukan analisis dan perancangan untuk mengolah informasi dan data yang telah didapat

d. Uji Coba dan Evaluasi

Pada tahap ini dilakukan uji coba program untuk mencari masalah yang mungkin timbul, mengevaluasi jalannya program, dan memperbaiki masalah yang mungkin muncul dalam program

e. Analisis Hasil Uji Coba

Pada tahap ini dihasilkan analisis dari serangkaian uji coba dan beberapa revisi, dan diharapkan perangkat lunak tersebut menghasilkan *output* yang diharapkan.

f. Pembuatan laporan Tugas Akhir

Pada tahap terakhir ini adalah proses penyusunan buku sebagai dokumentasi dari pelaksanaan Tugas Akhir. Buku laporan ini dibuat untuk memaparkan aplikasi yang telah dibangun agar memudahkan orang lain yang ingin mengembangkan aplikasi ini

1.7 Sistematika Penulisan

Dalam laporan tugas akhir ini, pembahasan disajikan dalam enam bab dengan sitematika pembahasan sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisikan tentang latar belakang masalah, perumusan masalah, batasan masalah, tujuan, manfaat, dan sistematika penulisan pembuatan tugas akhir.

BAB II TINJAUAN PUSTAKA

Pada bab ini menjelaskan tentang teori-teori pemecahan masalah yang berhubungan dan digunakan untuk mendukung dalam pembuatan tugas akhir.

BAB III ANALISIS DAN PERANCANGAN SISTEM

Bab ini dijelaskan tentang tata cara metode perancangan sistem yang digunakan untuk mengolah sumber informasi dan data yang dibutuhkan.

BAB IV IMPLEMENTASI

Pada bab ini menjelaskan implementasi dari program yang telah dibuat meliputi lingkungan implementasi, implementasi proses, implementasi antarmuka aplikasi.

BAB V UJI COBA DAN EVALUASI

Bab ini berisi pelaksanaan uji coba dan evaluasi dari pelaksanaan uji coba dari program yang dibuat.

BAB VI PENUTUP

Bab ini berisi kesimpulan dan saran untuk pengembangan aplikasi lebih lanjut dalam upaya memperbaiki kelemahan pada aplikasi guna untuk mendapatkan hasil kinerja aplikasi yang lebih baik.

DAFTAR PUSTAKA

Pada bagian ini akan dipaparkan tentang sumber-sumber literatur yang digunakan dalam pembutan laporan tugas akhir ini.